多項式の異なる素数を法とする根の分布について (解析的整数論の新しい展開)

AUTHOR(S):

北岡, 良之

CITATION:

北岡, 良之. 多項式の異なる素数を法とする根の分布について (解析的整数論の新しい展開). 数理解析研究所講究録 2009, 1639: 80-87

ISSUE DATE:

2009-04

URL:

http://hdl.handle.net/2433/140554

数理解析研究所講究録
第1639巻 2009年 80-87

多項式の異なる素数を法とする根の分布について

名城大学 北岡　良之 (Kitaoka Yoshiyuki)
Meijo University

$$f(x)=x^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0\in\mathbb{Z}[x]$$

を有理整数を係数とする monic な既約多項式とする。ここで考える問題は $f(x)$ を異なる素数で一次式の積に分解したときその根はどのように分布するかを調べよというものである。そのために素数の集合

$$Spl(f)=\{p\mid f(x) \bmod p \text{ is completely decomposable}\},$$

を考える。このとき $p\in Spl(f)$ に対し $r_1,\ldots,r_n$ $(r_i\in\mathbb{Z},\ 0\leq r_i\leq p-1)$ を $f(x)\equiv 0 \bmod p$ の根とする。そうすると $a_{n-1}+\sum r_i\equiv 0 \bmod p$ だから整数 $C_p(f)$ を

$$a_{n-1}+\sum_{i=1}^{n}r_i=C_p(f)p \tag{1}$$

で定める。このとき $C_p(f)$ について

Proposition 1 $f(x)=x+a$ $(a\in\mathbb{Z})$ とすると有限個の素数 p を除いて

$$C_p(f)=\begin{cases}1 & if\ a>0,\\ 0 & if\ a\leq 0\end{cases}$$

となる。

とやや自明ではない

Theorem 1 m を自然数とし $f(x)\in\mathbb{Z}[x]$ を *monic* な多項式で $\mathbb{Q}$ 上一次因子を持たないものとする。更に $f(x)=f_1(f_2(x))$ かつ $\deg f_2(x)=2$ となる $f_1(x),f_2(x)\in\mathbb{Q}[x]$ が存在するとする。このとき

$$C_p(f)=m\ (=\frac{1}{2}\deg f(x))$$

が有限個の素数 $p\in Spl(f)$ を除いて成り立つ。

が成立し、このふたつが例外的に $C_p(f)$ が求まる場合でこれら以外はランダムであると思われる。そこで素数 p が $Spl(f)$ を動くとき $C_p(f)$ がどのような値をとるか統計的に調べてみよう。いくつかの言葉を用意する。

以下 $f(x)$ は整数係数の多項式で monic とする。

(1) 正数 X に対し相対頻度を通常のように

$$Pr(c,f,X)=\frac{\#\{p\mid p\in Spl(f),p\le X,C_p(f)=c\}}{\#\{p\mid p\in Spl(f),p\le X\}}$$

と定める。

(2) 多項式 $f(x)$ に対して $\mathbb{Q}$ 上の多項式 $g(x),h(x)$ で

$$f(x)=g(h(x))$$

となるものがあるとする。このとき定数倍をして $g(x),h(x)$ は整数係数の monic な多項式と出来、更に $h(0)=0$ としてよい。この分解を退化分解と呼ぶことにする。退化分解として以下のような自明なものがある。

$$\begin{cases} g(x)=f(x), \\ h(x)=x, \end{cases} \qquad \begin{cases} g(x)=x+f(0), \\ h(x)=f(x)-f(0) \end{cases}$$

自明でない退化分解があるとき f は退化、そうでないときは非退化ということにする。f が退化のとき非自明な分解に対し $\deg h$ を退化次数ということにすると $f(x)=x^n$ の退化次数は n の真の約数全体である。また $\deg f(x)=\deg g(x)\cdot\deg h(x)$ だから退化次数は $\deg f(x)$ の真の約数、従って $\deg f(x)$ が素数なら $f(x)$ は非退化である。

(3) 整数全体から非負の実数への写像 p が度数分布表であるとは (i) 有限個の n についてのみ $p(n)\neq 0$, (ii) $p(n)=0$ if $n<0$, かつ (iii) $\sum_{n\in\mathbb{Z}}p(n)=1$ を満たすものをいう。平均 μ と分散 σ^2 を通常通り

$$\mu(p)=\sum_{n\in\mathbb{Z}}np(n),\quad \sigma^2(p)=\sum_{n\in\mathbb{Z}}n^2p(n)-\mu(p)^2$$

と定める。

度数分布表 p,q に対してその合成積 $p*q$ を

$$p*q(n)=\sum_{i+j=n}p(i)q(j),$$

と定めると $p*q$ もまた度数分布表で

$$\mu(p*q)=\mu(p)+\mu(q),\ \sigma^2(p*q)=\sigma^2(p)+\sigma^2(q)$$

となる。自然数冪 p^m を $p^1 = p$, $p^m = p * p^{m-1}$ で定める。
(4) 念のため Eulerian numbers $A(n,k)$ $(1 \leq k \leq n)$ の定義をしておこう。$A(1,1) = 1$ とし、以下帰納的に

$$A(n,k) = (n-k+1)A(n-1,k-1) + kA(n-1,k)$$

で定める。$1 \leq k \leq n$ でなければ $A(n,k) = 0$ とする。具体的な値は

$n \setminus k$	1	2	3	4	5	6	7	8	9
2	1	1							
3	1	4	1						
4	1	11	11	1					
5	1	26	66	26	1				
6	1	57	302	302	57	1			
7	1	120	1191	2416	1191	120	1		
8	1	247	4293	15619	15619	4293	247	1	
9	1	502	14608	88234	156190	88234	14608	502	1

Eulerian numbers による度数分布表 E_n $(n \geq 2)$ を

$$E_n(k) = \frac{A(n-1,k)}{(n-1)!}$$

によって定義する。例えば平均、分散は

$$\begin{cases} \mu(E_2) = 1, \\ \sigma^2(E_2) = 0, \end{cases} \quad \begin{cases} \mu(E_n) = n/2, \\ \sigma^2(E_n) = n/12 \end{cases} \quad \text{for } n \geq 3, \tag{2}$$

であり、$n = mr$ なら

$$\begin{cases} \mu(E_2^m) = m, \\ \sigma^2(E_2^m) = 0, \end{cases} \quad \begin{cases} \mu(E_r^m) = n/2, \\ \sigma^2(E_r^m) = n/12 \end{cases} \quad \text{for r} \geq 3$$

となっており、$r = 2, 3$ に対しては

$$E_2^m(k) = \begin{cases} 1 & \text{if } k = m, \\ 0 & \text{otherwise}, \end{cases}$$

$$E_3^m(k) = \begin{cases} 2^{-m}\binom{m}{k-m} & \text{if } m \leq k \leq 2m, \\ 0 & \text{otherwise} \end{cases}$$

である。これらは対称で単峰、即ち $E_r^m(k) = E_r^m(rm-k)$ for $^\forall k \in \mathbb{Z}$ かつ $E_r^m(1) \leq E_r^m(2) \leq \cdots \geq E_r^m(mr-2) \geq E_r^m(mr-1)$。

1 既約な場合

以上の準備の下に我々の予想を述べよう。

Conjecture 1 $f(x) \in \mathbb{Z}[x]$ を *monic* な次数 $n(\geq 2)$ の非退化既約多項式とする。このとき任意の自然数 c に対して

$$Pr(c, f) = \lim_{x \to \infty} Pr(c, f, x)$$

が存在し、$E_n(c)$ に等しい。言い換えると度数分布表 $Pr(f) : c \mapsto Pr(c, f)$ は E_n に一致する。

Remark 1 *[K2]* の予想 *1.7* は以下の様に修正すべきである。それはそこでの退化次数はここで言う退化次数の最小値と定義していたが後で触れるようにそれは不適切であることが判明したからである。

> $f(x) \in Z[x]$ を *monic* な既約多項式で次数 $n\,(\geq 3)$ とする。また 2 は退化次数ではないとする。そのとき $Pr(f) : c \mapsto Pr(c, f)$ で定義される度数分布表は以下を満たす。
>
> $$\mu(Pr(f)) = n/2,\ \sigma^2(Pr(f)) = n/12,$$
> $$Pr(k, f) = Pr(n-k, f)\ for\ ^\forall k,$$
> $$Pr(1, f) \leq Pr(2, f) \leq \cdots \geq Pr(n-2, f) \geq Pr(n-1, f)\ 。$$

さて平均が $1/2$、分散が $1/12$ を持つものとして $[0, 1)$ での一様分布が知られていて、$x_1, \cdots, x_n$ を独立な $[0, 1)$ 上の一様分布とすると $x_1 + \cdots + x_n$ の平均、分散はそれぞれ $n/2$、$n/12$ である。このことを考慮すると上の予想は何か背後に一様分布するものがあることを示唆しているように見える。思いつくものをあげると

Conjecture 2 $F = \mathbb{Q}(\alpha)\,(\neq \mathbb{Q})$ を代数体で α は代数的整数とする。k を非負整数とする。F で完全分解する素数 p に対し p の上にある素イデアルを $\mathfrak{p}$ と表す。$F_{\mathfrak{p}} = \mathbb{Q}_p$ で

$$\alpha = c_{\mathfrak{p}}(0) + c_{\mathfrak{p}}(1)p + \cdots \quad (c_{\mathfrak{p}}(i) \in \mathbb{Z}, 0 \leq c_{\mathfrak{p}}(i) < p)$$

と展開すると、点 $(c_{\mathfrak{p}}(0)/p, c_{\mathfrak{p}}(1)/p, \cdots, c_{\mathfrak{p}}(k)/p)\,(\in [0, 1)^{k+1})$ は $p, \mathfrak{p}$ がすべての完全分解する素数とその上にあるすべての素イデアルを動くとき一様分布する。

Remark 2 αが二次の代数的整数で$k=0$なら予想2は正しい([DFI],[T])。また予想2から予想$\mu(Pr(f))=n/2$も従う。

一様分布の観点から幾つかの注意を述べる。以下$f(x)\in\mathbb{Z}[x]$はmonicかつ既約で次数は2以上とする。

1. 定義(1) $\sum r_i/p = C_p(f) - a_{n-1}/p$から点$(r_1/p,\cdots,r_n/p)$は$[0,1)^n$で一様分布しない。

2. 実数xに対しxより小さくない最小の整数を$\lceil x\rceil$で表す、即ち$\lceil x\rceil - 1 < x \leq \lceil x\rceil$とし、更に実ベクトル$\boldsymbol{x}=(x_1,\cdots,x_a)\in\mathbb{R}^a$に対し$\lceil\boldsymbol{x}\rceil = \lceil x_1+\cdots+x_a\rceil$と置く。このとき$E_n(k)=A(n-1,k)/(n-1)!$は次の集合
$$S_k = \{\boldsymbol{x}\in[0,1)^{n-1} \mid \lceil\boldsymbol{x}\rceil = k\}$$
の体積である。従って$\boldsymbol{x}_m\in[0,1)^{n-1}$が一様分布するなら
$$\lim_{m\to\infty}\frac{\#\{m \mid \boldsymbol{x}_m\in S_k\}}{m} = E_n(k)$$
である。

3. $f(x)\equiv 0 \bmod p$のnケの局所解$r_1,\cdots,r_n$に対し、有限個のpを除いて「そのうちの任意の$n-1$個に対し
$$(r_1/p,\cdots,r_{n-1}/p)\in S_k$$
が成り立つこと」と「$C_p(f)=k$が成り立つこと」とは同値である。従って、2.を考慮に入れるとσが集合$\{1,2,\cdots,n\}$の置換をすべて動いて均された点達$(r_{\sigma(1)}/p,\cdots,r_{\sigma(n-1)}/p)\in[0,1)^{n-1}$は一様分布であろうし、予想にEulerian numbersが現れる理由でもあろう。

4. 次に$f(x)=g(h(x))$と退化する場合を考える。
$$\begin{aligned} g(x) &= x^m + a_{m-1}x^{m-1} + \cdots \quad (m>1),\\ h(x) &= x^r \ + b_{r-1}x^{r-1} \ + \cdots \quad (r>1), \end{aligned}$$
と置くと
$$a_{m-1} = mb_{r-1}$$
となり、素数$p\in Spl(f)$に対して局所解を以下のように分類する：
$$\{r_i \mid f(r_i)\equiv 0 \bmod p\} = \cup_{i=1}^{m}\{r_{i,1},\cdots,r_{i,r}\},$$

ここで $r_{i,j}$ は

$$h(r_{i,j}) \equiv {}^{\exists}s_i \bmod p \quad (1 \leq {}^{\forall}j \leq r),\ g(s_i) \equiv 0 \bmod p$$

を満たすように定める。このとき $C_p(f) = \sum_{i=1}^{m} C_p(h(x) - s_i)$ となる。また

Proposition 2 $\{r_{i,1}, \cdots, r_{i,r}\}$ から任意に選択した $r-1$ ヶに対し

$$C_p(h(x) - s_i) = \lceil (r_{i,1} + \cdots + r_{i,r-1})/p \rceil$$

が有限個の p を除いて成り立つ。

もわかる。従って

$$S_{m,r}(k) = \{(\boldsymbol{x}_1, \cdots, \boldsymbol{x}_m) \mid \boldsymbol{x}_i \in [0,1)^{(r-1)}, \sum_{i=1}^{m} \lceil \boldsymbol{x}_i \rceil = k\}$$

と置くと $vol(S_{m,r}(k)) = E_r^m(k)$ であることに注意すると、点

$$(\boldsymbol{r}_1(\mu, \sigma_1), \cdots, \boldsymbol{r}_m(\mu, \sigma_m)) \in [0,1)^{m(r-1)} \tag{3}$$

(但し $\boldsymbol{r}_k(\mu, \sigma_k) = (r_{\mu(k),\sigma_k(1)}/p, \cdots, r_{\mu(k),\sigma_k(r-1)}/p)$ と置く) は μ が $\{1, 2, \cdots, m\}$ のすべての置換、σ_i が $\{1, 2, \cdots, r\}$ のすべての置換を動くとき一様分布すれば $Pr(f) = E_r^m$ となる。

退化分解が唯一つで2が退化次数ではないとき $Pr(f) = E_r^m$ は実験的には正しい。従って (3) の点たちも一様分布しそうである (少なくとも実験的には)。

しかし $\deg f = 12$ のときの例が示すように複数の退化分解を持つときは状況はよくわからない。多次元の点が一様分布するすることを実験的に自分で納得できるにはかなりのデータが要り、今の場合とても普通のパソコンでは無理である。しかし上の2番目の注意から多次元の点が一様分布すればその点の要素の和の分布は Eulerian だから要素の和の分布が Eulerian かどうかをチェックすることによって多少の観察は出来る。12次の多項式

$$\begin{aligned} f &= y^4 - 9y^3 + 27y^2 - 27y + 3 \quad (y = x^3) \\ &= y^3 + 3 \qquad\qquad\qquad\qquad\quad (y = x^4 - 3x) \end{aligned}$$

の Pr は E_3^4 でも E_4^3 でもない。しかし

$$f = x^{3\cdot5} + 2,\ x^{3\cdot7} + 2,\ x^{5\cdot7} + 2,\ x^{3\cdot5\cdot7} + 2$$

などに対しては夫々退化次数の最小値 $3, 3, 5, 3$ を r とし $m = n/r$ ($n = \deg f$) $g(x) = x^m + 2$, $h(x) = x^r$ とおくと実験的には $Pr = E_r^m$ である。しかし (3) の点は一様分布しない。それは z を $\mathbb{Z}/p\mathbb{Z}$ の 1 の n 乗根とし a を $f(x) \equiv 0 \bmod p$ のひとつの根とすると他の根は az^k と書け、4. の $\{r_{ij} \mid 1 \leq j \leq r\}$ として $r_{ij} = az^{(i-1)+m(j-1)}$ $(i = 1, \cdots, m, j = 1, \cdots, r)$ が取れる。また $(m, r) = 1$ だから $az^{r(i-1)}$ $(i = 1, \cdots, m)$ は r 乗がすべて異なる。よって (3) の点の一成分として $\boldsymbol{r}_k(\mu, \sigma_k) = (az^{r\cdot0}/p, az^{r\cdot1}/p, \cdots, az^{r(m-1)}/p)$ を取るとそれらの成分の和は整数になるからである。近似的には ($p < 10^9$) $Pr = E_r^m$ であるが一様分布していないのだからデータ不足ではないかといわれても反論できるだけのデータを集めることは難しい。

また上の 12 次の多項式に対しては (3) の代わりに

$$(\boldsymbol{r}_1(\mu, \sigma_1), \cdots, \boldsymbol{r}_{m-1}(\mu, \sigma_{m-1})) \in [0, 1)^{(m-1)(r-1)}$$

は一様分布しそうであるが $\boldsymbol{r}_m(\mu, \sigma_m)$ の一点でも付け加えると一様分布しないようである。

一般に退化分解の意味もわからないし、複数の退化分解を持つときそれらの関係もわからない。

実験データや多項式が可約その他のときについては [HKKN, K2, K3] をご覧頂きたい。

なおこの研究の発端は [K1, HKKN] の分数の小数展開である。

参考文献

[DFI] W. Duke, J.B. Friedlander and H. Iwaniec, *Equidistribution of roots of a quadratic congruence to prime moduli,* Ann. of Math., 141(1995), 423-441.

[HKKN] T. Hadano, Y. Kitaoka, T. Kubota, M. Nozaki, *Densities of sets of primes related to decimal expansion of rational numbers*, Number Theory: Tradition and Modernization, pp. 67-80, W. Zhang and Y. Tanigawa, eds. ©2006 Springer Science + Business Media,Inc.

[K1] 北岡良之, 代数入門, 金苑書房 2004

[K2] Y. Kitaoka, *A statistical relation of roots of a polynomial in different local fields*, to appear in Mathematics of Computation (January 2009).

[K3] Y. Kitaoka, *A statistical relation of roots of a polynomial in different local fields II*, hopefully to appear in Proceeding of Japan-China Seminar on Number Theory.

[T] Á. Tóth, *Roots of Quadratic congruences,* Internat. Math. Res. Notices 2000, 719-739.